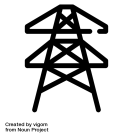
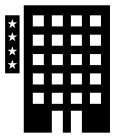

i-thic
The Edge is the New Centre

Agenda



Introduce OISP, the technology that underpins Iothic's IIOT communications platform



Understand how it works, how it is different and what benefits it brings

Agree on next steps

What problems Iothic has solved

The IoT Promise

00 billions of connected devices & vast volumes of data* leveraged by advanced AI to orchestrate industrial and human systems

Reduce errors, waste, cost and deliver tailored outcomes to … **save lives, reduce pollution, improve productivity and deliver value****

Use-cases include:
logistics – asset tracking
transport – congestion management
cities – energy and pollution reduction
agri – smart irrigation
industry – production line automation

**41bn devices, ~80ZB data by 2025*
***$11tn consumer surplus by 2025*
Sources: IDC June 2019, McKinsey MGI June 2015

The Impediments

Security – Cyber attacks increasing each year, IOT edge is the weak link**

Interoperability – IOT must connect many different devices, on different platforms so that they can connect seamlessly

Legacy infrastructure – Industry 4.0 must integrate with existing devices which have old technology and low compute power

Issues with current security solutions:
- rely on CA/TTP – management challenge for edge devices, repository of authentication and relies on third party
- assume cloud connectivity – not always available and increases attack surface
- hook the client with proprietary HW/SW

***34m IOT attacks recorded in 2019*
Sources: SonicWall 2020 Cyber Threat Report

The solution: Iothic's OISP

Iothic has developed the first of its kind, a **decentralised IIOT communications platform** that let's any thing talk to any thing securely. At its heart is the **Open IOT Security Protocol "OISP"** - a radical new approach built on 10 years of cryptographic research at Oxford University by Professor W Roscoe

Post-quantum authentication and data in-transit encryption from the edge inwards. Real-time, without need for cloud connectivity, or Certificate Authority - a full PKI replacement and elimination of the 'security key management' challenge

Current sector engagement includes defence, smart city, upstream oil, UK, SEA, ANZ

www.iothic.io founded by Chris Autry in 2017

A high level explanation of how OISP works

Fully decentralised, interoperable framework

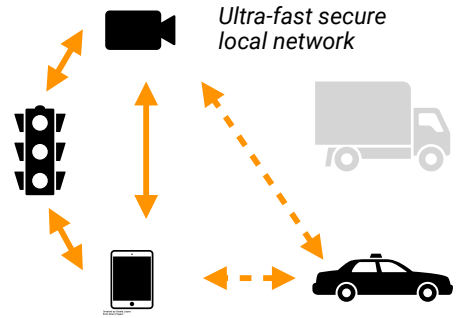
Peer to Peer communication, not client-server
Self-contained - no third party
Set and forget - fresh keys generated locally every session; identity authenticated locally every session
Forward and backward compatible

Quantum resistant security from the edge inwards

Every session conducts fresh device authentication and uses fresh (one-time) payload encryption keys
All keys are strong (NTRU and AES 256)
Strong hashes (SHA3 Keccak)
Only hashed data exchanged during authentication
Unique nonces
Local entropy
Secure against known quantum attacks (Shor, Grover algorithms)

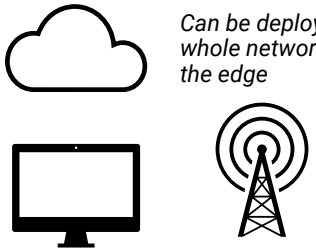
Technology and footprint agnostic

Integral to the device
Works alongside existing technology
All comms and transport layers
Integration and legacy replacement not necessary



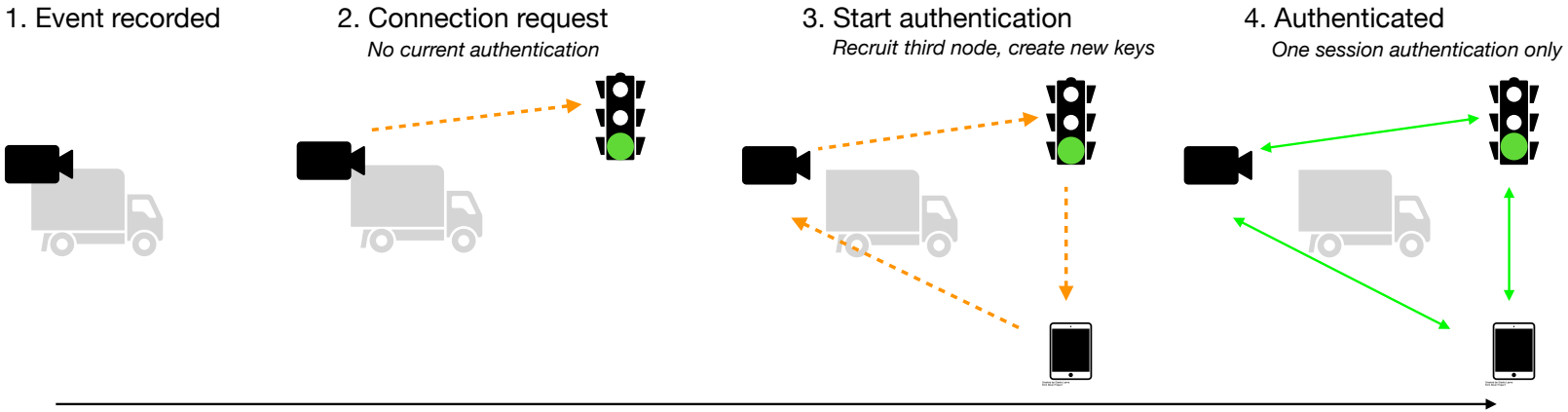
Protocol is integral to device
Compatible with legacy and future technology

No transmission delay or dropouts
No need for cloud or server connectivity
100% local and secure



Can be deployed through the whole network, not just at the edge

Fast, edge-based, three node authentication



Steps 1 - 4 All using Short Time / One Time Cryptography

Authentication is fresh each time

Steps are encrypted with one session only keys

Scheme based on hash proof of device properties

Third node used as independent facilitator & verifier

Process effected entirely at the edge

No repository of data and no property data transmitted

Encryption key is one session only

OISP is unique

OISP secure interoperability		Other market offerings - typical components
Authentication steps are 100% local to linked devices	⟷	CA/PKI using trusted third party
Authentication is an encrypted multi-step process involving unique device properties	⟷	Single step token or password match
Devices use local entropy to create keys for hash and encryption	⟷	Asymmetric keys created by third party
Fresh keys, created on linked devices, are used for every session	⟷	Multi-session keys
Backwards and forwards compatible	⟷	Require integration on different technologies

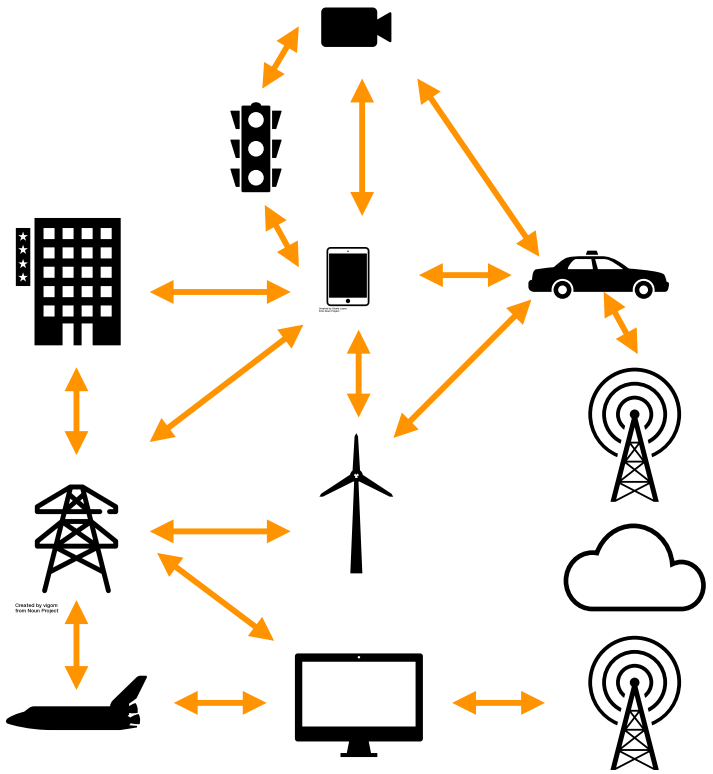
The benefits of OISP

More secure networks
- Vulnerable edge secure
- Full network quantum secure
- No certificate honey-pots or password repositories

Lower cost
- Replacement of CA/PKI
- Eliminated key management processes
- Reduced risk of loss / insurance cost
- Better Process Stage Interaction (Production & Supply)
- Reduce Core Network Coms (Decentralisation)
- Reduced integration costs as a result of backward & forward compatibility

Improved data control / privacy
- Ability to prevent third-party meta-data management
- Potential for 100% own core system control
- Can be managed entirely within own firewall

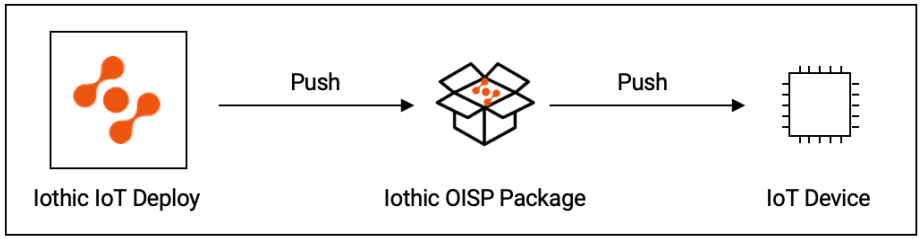
Faster deployment of smart networks
- Impediments to IIOT overcome
- Interoperability delivered
- Risks of data theft and device repurposing minimised
- Able to integrate and trust new networks rapidly



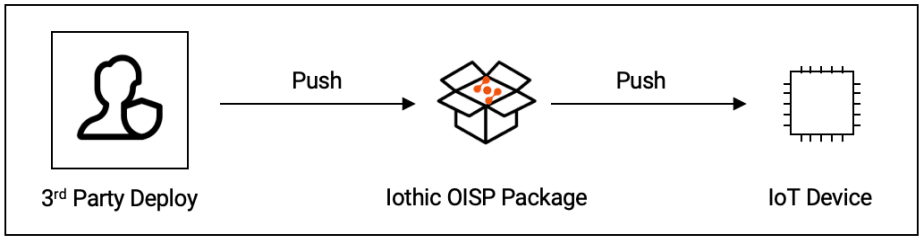
iPad by Gisela Leyva from the Noun Project
Tower by vigorn from the Noun Project

Deployment options

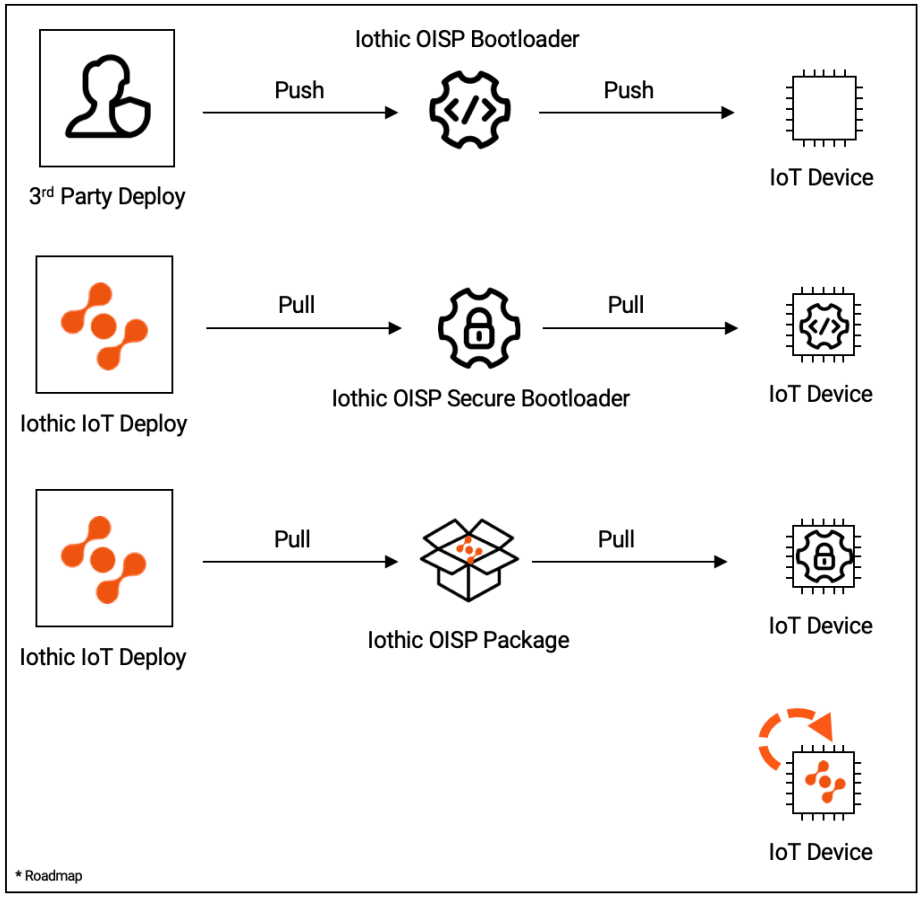
Option 1



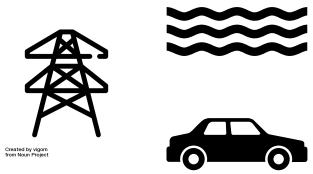
Option 2



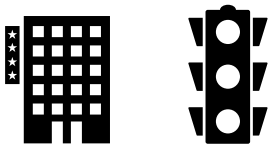
Option 3*



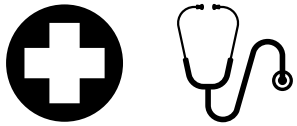
Use-cases



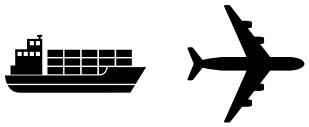
Critical national infrastructure
- Power and gas grid maintenance
- Water security management
- Major highways incident management



Smart infrastructure
- Building environmental control
- City traffic management
- Street safety



Healthcare
- Emergency services management
- Field diagnostics and primary care coordination
- Medical device management



Ports and border entry
- Container tracking
- Passenger movement monitoring
- Incident response management

Example attacks OISP would prevent

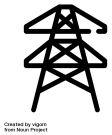
Intercept and change payload data
- ***Disguise water quality contamination readings***
- ***Create fake critical incident flags***

Spoof sensors to take control
- ***Influence traffic management***
- ***Influence building management***

Intercept to learn private information
- ***Decrypt sensitive data***
- ***Stop devices operating safely***

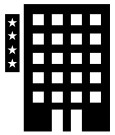
Intercept and spoof
- ***Falsify container location report***
- ***Intercept and read movement reports***

Next steps



Select use-case for test-case

Note: We are in design stage of test-cases for water network and remote oil extraction



Engage potential end-user

This is to ensure the test-case is a valid prototype for real-world deployment

Deliver demonstration / proof of concept

We estimate 6-8 weeks including rigorous attack vector tests and interoperability

IOTHIC LTD

BACKGROUND

-Collaboration with Oxford University Computer Science Division

-Technology produced as a result of over 10 years of cryptographic research

-Underpinning research developed for the Ministry of Defence (MoD) and the US Navy-Universal security protocol developed specifically for edge computing, first of its kind

COMPANY FACTS

-UK registered entity

-25 FTE Employees

KEY PEOPLE

Christopher Autry, CEO (BA University of Chicago; MSc Oxford University)

Prof. William Roscoe, CSO (BA,Ph.D, Oxford University)

Dr Michael Penington, Director (BA,Ph.D Oxford University)

Dr Mykhailo Magal, CTO (MSc.,Ph.D, Kiev National University)

Wayne Henderson, EVP (BA, MSc, MBA, Oxford University, Lancaster University, Macquarie University)

Anthony Hogan VP (BSc (Hons) University College)

Mark Slinger VP Product (BSc (Hons) Newcastle University)

-

Oxford University and UK Government backing, fully funded by Longwall Ventures

www.iothic.io